DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY

FREQUENTLY ASKED HIPAA QUESTIONS (FAQ)

June 2004

Navy Medicine's Frequently Asked HIPAA Questions (FAQs)

Topic

Appointment Reminders

Back to the Top

Q: May Clinics leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments?

A: Yes. Leaving messages on a patient's answering machine is not prohibited. However, to reasonably safeguard the individual's privacy, take precautions to limit the amount of information disclosed by leaving only the facility name and number, other information necessary to confirm the appointment, or alternatively, leave a contact number and ask the patient to call back. Professional judgment should be used to assure that such disclosures are in the best interest of the patient and to limit the information disclosed. Automated systems should be configured to accommodate requests for confidential or restricted communications.

Athletes and HIPAA

Back to the Top

Q: Can Protected Health Information (PHI) be released for staff members involved in off-duty athletics?

A: Prior to releasing PHI on staff members involved in athletics, the patient's (athlete's) written authorization is required. The PHI that is released is subject to the "minimum necessary provisions" of the HIPAA Rule.

The following link has some information regarding sports industry and release of athlete's PHI: http://www.hipaadvisory.com/views/privacy/prosports.htm.

Business Associate Agreements

Back to the Top

Q: Is a business associate agreement required with organizations or persons where inadvertent contact with PHI may result?

A: A business associate agreement is not required with persons or organizations whose functions, activities, or services do not involve the use or disclosure of PHI, and where any access to PHI by such persons would be incidental, if at all. Incidental disclosures are permitted by the HIPAA Privacy Rule. For example, janitorial contractors that clean the offices or facilities of a covered entity are not business associates because the work they perform does not involve the use or disclosure of PHI. Any disclosure of PHI in the performance of their duties is limited in nature,

occurs as a by-product of the services, and could not be reasonably prevented. However, a confidentiality agreement may be indicated.

When an organization is hired to do work for a covered entity where disclosure of PHI is not limited in nature (such as routine handling of medical/dental records or shredding of documents containing PHI), that entity would most likely be a business associate. However, when such work is performed under the direct control of the covered entity (e.g., on the covered entity's premises), the Privacy Rule permits the covered entity to treat the service as part of its workforce, and a business associate agreement is not required.

Command HIPAA Instruction and Policy Back to the Top

Q: Should MTFs/DTFs create local HIPAA Privacy Manuals or Instructions?

A: The DoD Regulation 6025.18R provides the overarching guidance on HIPAA within the Military Health System (MHS). This Regulation and the final HIPAA Rule should be used as references to integrate local Policies and Procedures. Although there is no requirement to have a Manual or Instruction outlying your specific policies, it is strongly recommended.

Critical HIPAA Areas of Concern Back to the Top

Q: What are some of the critical components of the HIPAA Rule that I need to focus my attention on?

A: Disclosure Tracking, HIPAA-related complaints, staff misuse of PHI and Application of Minors Rights are some of the significant areas where Policies and Procedures should be prepared and staff trained on required protocols. This list is not all-inclusive and serves as examples of critical areas of focus; however, local concerns will dictate the priorities for compliance at each MTF/DTF.

Electronic Mail

Back to the top

Q: Can I still send PHI in electronic mail (email)?

A: The HIPAA Privacy Rule does not prohibit sending PHI in electronic mail, but does require reasonable and necessary precautions to avoid inadvertent disclosure. In addition to confirming the recipient's address and authority to receive the information, senders should send only the information necessary to accomplish the purpose, ensure the transmission is by the most secure means available, and alert recipients that the message is subject to privacy restrictions by including a disclaimer statement. Local policies may provide additional guidance on use of PHI in e-mail.

Q: What e-mail disclaimer should be used for outgoing mail?

A: TMA has provided the following text for use on any e-mail:

"This document may contain information covered under the Privacy Act, 5 USC 552(a), and/or the Health Insurance Portability and Accountability Act (PL 104-191) and its various implementing regulations and must be protected in accordance with those provisions. Healthcare information is personal and sensitive and must be treated accordingly. If this correspondence contains healthcare information, it is being provided to you after appropriate authorization from the patient or under circumstances that don't require patient authorization. You, the recipient, are obligated to maintain it in a safe, secure and confidential manner. Redisclosure without additional patient consent or as permitted by law is prohibited. Unauthorized redisclosure or failure to maintain confidentiality subjects you to application of appropriate sanction. If you have received this correspondence in error, please notify the sender at once and destroy any copies you have made."

Facility Retrofits

Back to the Top

Q: Does the HIPAA Privacy Rule require hospitals or dental clinics to be retrofitted, to provide private rooms, and soundproof walls to avoid any possibility that a conversation is overheard?

A: No, the Privacy Rule does not require any type of structural changes to a facility. However, covered entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. This standard requires that covered entities make reasonable effort to prevent uses and disclosure not permitted by the Rule. They must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures.

Fax Usage

Back to the Top

Q: Can a clinic fax patient medical information to another clinic or provider's office?

A: The HIPAA Privacy Rule permits physicians to disclose PHI to another health care provider for treatment purposes. This can be done by fax or by other means. Covered entities must have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of PHI that is disclosed using a fax machine. Examples of measures that could be reasonable and appropriate in such a situation include the sender confirming that the fax number to be used is in fact the correct one for the other clinic or provider's office, and placing the fax machine in a secure location to prevent unauthorized access to the information.

Disclosure Tracking

Back to the Top

Q: Is there a requirement to account for disclosures to Military Commanders?

A: Yes, unless the disclosure is considered part of treatment, payment, or health care operations (TPO), it should be documented and accounted for using the Protected Health Information Management Tool (PHIMT).

HIPAA Refresher Training

Back to the top

Q: Has TMA developed Training Modules to be used for Annual HIPAA Refresher Training?

A: Yes. TMA has developed HIPAA Refresher Training Modules that will be available for Command use in May 2004. These Modules will be released based on an individual's job position. The schedule for release of this training is indicated below. Additionally, if Commands identify other HIPAA Training Requirements regarding local Policies and Procedures, they can supplement the TMA Training as needed locally, and tracking would also be done at the local level.

HIPAA Privacy Refresher Training Rollout

Rollout Month	Job Position
May 2004	Senior Executive Staff, Volunteers, Medical Records/Patient Admin, and IM/IT
July 2004	Nursing
September 2004	Ancillary Clinical
November 2004	Admin Support Services and Facility Support Services
January 2005	Business/Finance and Provider

Inpatient Records Back to the Top

Q: Is there a requirement to place the NOPP Acknowledgement label on Inpatient Records?

A: HIPAA requires that the Notice of Privacy Practices (NOPP) be provided to the patient on the first occasion they present for services. If the patient presents to an outpatient clinic and their medical records are with them, the policy is to ensure the NOPP label is affixed to the back of that record and that the patient has acknowledged receipt of the NOPP. If the patient is to be admitted to the MTF, the Admission's staff should ask if they have received the NOPP; if not, an NOPP is provided, but a label is not required on the Inpatient medical record.

Covered Entity Workforce Back to the Top

Q: How is the term "workforce" defined?

A: Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

JCAHO and HIPAA

Back to the Top

Q: From recent Joint Commission and Navy IG Survey, how have activities been evaluated?

A: In evaluating Commands during a JCAHO/IG Survey, the concept of "due diligence" has been exercised and Commands have been assessed on their ability to demonstrate the safeguarding of PHI, as well as having staff members trained. In a recent IG Inspection, the Inspector used the FCG Site Visit Executive Summary Report as a baseline to determine the current status of the Command and progress made since the site visit.

Mental Health

Back to the Top

Q: Can a Commanding Officer request mental health PHI on an active duty member attached to his/her Command or does the member need to sign an authorization for disclosure?

A: Yes. If in the Commanding Officer's opinion the disclosure is required to ensure the proper execution of the military mission, the Military exclusion would apply and no authorization would be required by the active duty member. Command prerogative to obtain PHI based on operational necessity does not apply to "Psych Notes" and "Substance Abuse". Further guidance should be obtained before disclosing PHI in either of these areas.

Q: May mental health providers or other specialists provide therapy to patients in a group setting where other patients or family members are present?

A: Yes. The Office of Civil Rights states that disclosures of PHI in a group therapy setting are treatment disclosures and may be made without an individual's authorization. Furthermore, the HIPAA Privacy Rule generally permits a covered entity to disclose PHI to a family member or other person involved in the patient's care. Where the patient is present during the disclosure, the covered entity may disclose PHI if it is reasonable to infer from the circumstances that the individual does not object to the disclosure.

NOPPs/Privacy Forms Back to the Top

Q: Where can I order HIPAA Privacy Notice of Privacy Practices and related DoD HIPAA Forms?

A: You can go to the TMA Website at: http://tricare.osd.mil/SMART/ to order the MHS NOPP and related HIPAA Privacy Forms.

Officers of the Day Back to the Top

Q: Should Command Duty Officers and/or Officers of the Day have access to PHI?

A: Each Command should determine who needs to be present at "Morning Report", and what, if any, PHI is required to be discussed. In the event the Command determines the need to discuss PHI, only those having a need to know should be present and every effort should be made to de-identify the PHI of the patient being discussed. Depending on the patient category, different rules may apply, and it is recommended that each Command consult their HIPAA Privacy Officer for further guidance.

Other Resources Back to the Top

Q: What other related Web Sites can I search for FAQs?

A: You can find answers to a variety of HIPAA-related topics at the following Web Sites:

TMA FAQs can be found at:

http://tricare.osd.mil/tmaprivacy/hipaa/hipaacompliance/faqs/index.htm

U.S. Department of Health & Human Services FAQs can be found at:

http://answers.hhs.gov/cgi-bin/hhs.cfg/php/enduser/std_alp.php?p_sid=ySEcB8Eg&p_lva=&p_li=&p_page=1&p_cat_lvl1=7&p_cat_lvl2=%7Eany%7E&p_search_text=&p_new_search=1

Clinic Check-In

Back to the Top

Q: May clinics use patient sign-in sheets or call out the names of their patients in waiting rooms?

A: Yes. The Office of Civil Rights put out the following guidelines: Covered entities, such as clinics, may use patient sign-in sheets or call out patient names in waiting rooms, so long as the information disclosed is appropriately limited. The HIPAA Privacy Rule explicitly permits the incidental disclosures that may result from these types of practices. However, these types of incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem for which the patient is seeing the provider).

Peer Review Proceedings

Back to the Top

Q: Can a patient's PHI be disclosed during the course of Peer Review proceedings?

A: Yes. Peer Review proceedings are considered part of Treatment, Payment, and Operations (TPO) under the HIPAA Privacy Rule and as such, PHI can be disclosed without a patient's authorization for such purposes. Additionally, an attorney representing a physician before a Peer Review Panel at a Naval MTF is entitled per BUMEDINST 6320.67A (enclosure (7)) to receive (at least 10 days prior to the hearing) "copies of all documents the panel will receive and consider" and has the right to present (relevant) evidence. The DoD HIPAA regulation (DoD 6025.18-R) authorizes the MTF to use or disclose PHI for healthcare operations (section C1.2.2), which includes Peer Review Proceeding (per section DL1.1.13.2). In the case that an attorney is retained, it is imperative to have sufficient documentation to establish the attorney-client relationship prior to the release of information; and the attorney should be informed of the restrictions under 10 USC 1102 that prohibit further release of any information gathered in the process. The Peer Review process is privileged information under 10 USC §1102 and cannot be released except as allowed under the statute. As a rule, you should confer with JAG in advance of providing PHI to support the proceedings.

Prescription Pick-up

Back to the Top

Q: Can a patient have a family member or friend pick up his/her prescription?

A: Based on the guidance provided by the Office of Civil Rights in December 2002, an authorization is not required for a family member or patient's representative to pick up a prescription. In doing so, it is implied that the patient has given authorization to pick up the prescription. However, each Command has the right to implement a more restrictive policy if they chose to do so. The Pharmacist is permitted to use professional judgment and experience with common practice to make reasonable inferences of the patient's best interest in allowing a person, other than the patient, to pick up a prescription.

Security Training

Back to the Top

Q: Is there a plan to have HIPAA Security Training anytime in the near future?

A: HIPAA Security training is currently being discussed at the TMA and Service levels, and the training guidance will be announced soon.

Staff Communications

Back to the Top

Q: Can health care providers engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard?

A: Yes. According to the Office of Civil Rights, the HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requiring covered entities to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that providers' primary consideration is the appropriate treatment of their patients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, high-quality care. The Privacy Rule also recognizes that overheard communications in these setting may be unavoidable and allows for these incidental disclosures.

Training Programs

Back to the Top

Q: Do the HIPAA Privacy Rule's minimum necessary requirements prohibit medical residents, medical students, nursing students, and other medical trainees from accessing patient's medical information in the course of their training?

A: No. According to the Office of Civil Rights, the definition of "health care operations" in the Privacy Rule provides for "conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers." Covered entities can shape their Policies and Procedures for minimum necessary uses and disclosures to permit medical trainees access to patients' medical information, including entire medical records.

Training—Using another Vendor's Tool

Back to the Top

Q: Can another product, such as the Healthstream training module, be substituted for the TMA Training Tool? Also, are there any other ways that training can be accomplished other than every staff member logging in individually?

A: The TMA HIPAA Training Tool (LMS) is to be used for all HIPAA Training within the MHS. Other locally developed or procured Training Tools or databases can be used, but HIPAA LMS is the Tool used to track training completion throughout the Military Health System.

White Boards

Back to the Top

Q: What is the policy regarding the use of White Boards on Inpatient Wards?

A: HIPAA does not prohibit the use of White Boards. It allows for these types of "incidental disclosures" as long as you can demonstrate that reasonable safeguards were applied to limit incidental disclosure.

Q: Are Providers prohibited from maintaining medical records at bedside or outside of exam rooms?

A: No. The Office of Civil Rights has stated that covered entities must implement reasonable safeguards to protect a patient's privacy. Additionally, covered entities must reasonably restrict how much information is used and disclosed, where appropriate, as well as who within the entity has access to PHI. Covered entities must evaluate what measures make sense in their environment and tailor their practices and safeguard to their particular circumstances.